REMARKS

It is believed that the case is now allowable.

The Office Action raised issues under 35 U.S.C. §112 which have now been addressed.

The proposed amendment to the claims and the canceling of Claim 76 is further for purposes of eliminating issues on appeal under 37 C.F.R. §1.116 if the Examiner does not believe the present application is now allowable.

Basically, each of the claims have been rejected as either anticipated or rendered obvious by cited sections of the *Schneier* "Applied Cryptology, Second Edition" reference.

The *Schneier* reference discusses encryption systems on Pages 180-182 and more particularly the capacity of controlling and storing keys for an encryption system. The Office Action contended on Page 3, that *Schneier* discloses:

> "Switching between the key storage medium and the password to obtain
> the key information (Page 182, Paragraph 4) which obtains the key from
> both the memory and the portable ROM key in order to decrypt the cipher
> text."

It is believed that this quote is erroneous and that the Office Action may have been referring to Page 181, fourth paragraph, where a single key was split into two halves. One half of a key was stored in the terminal and the other in a ROM key. This increased security since if one of the key halves was lost it would not compromise the other key half. Thus, the user must unite both halves of the key to form a single key to be able to decrypt the ciphered text.

Since this is a critical point supporting an alleged teaching of the "switch unit" set forth in our claims, it is requested that if the Office Action is referring to some other paragraph, that applicant be given an opportunity to respond since it is believed that there has been an erroneous citation in the Office Action.

62478.9100\PROCE\IRV\445321

10

Our switch unit defines a specific manner of operation wherein a key can be secured from one of two sources independently and either form of the key can be utilized to enable a decryption unit to decrypt the encrypted file key, and accordingly, decrypt the ciphered text using the decrypted file key. Such an arrangement may not have the higher security taught in the *Schneier* reference, but it serves the purpose of permitting a user to have two methods to obtain key information.

The present invention of Claim 17 is characterized by "a switch unit (a) including a first key obtaining unit operable to receive an input of a second password from the user and decrypt the encrypted key stored in the memory unit using the received second password to generate decrypted key information, and a second key obtaining unit operable to read the original key information from the key storage medium loaded in the file decryption apparatus, and (b) is operable to obtain either the original key information or the decrypted key information by one of the first key obtaining unit and the second key obtaining unit." The *Schneier* reference does not disclose such a "switch unit."

With our invention, if a user has a key storage medium, the user only has to load the key storage medium in the file management apparatus. This is easier and more convenient for the user than inputting a password.

On the other hand, if the user fails to prepare a key storage medium or loses the same, the user can still input a password to generate the key information. For example, Figure 2, with separate password input units 101 and 301 are certainly not shown nor taught in the *Schneier* reference. See also the flow chart operation of our switch unit S141, S142 in Figure 5, with another password entry in Steps S144 via input unit 301.

11

As understood from this, the present invention provides the user with two methods, from which the user can select one, for obtaining the key information. The present invention, therefore, brings about a highly advantageous effect of providing a file management apparatus that obtains a key necessary for decrypting a cipher text, in a safe and highly convenient manner for the user.

As noted above, Page 181, Paragraph 4 of the *Schneier* reference states: "This technique is made more secure by splitting the key into two halves, storing one half in the terminal and the other half in the ROM key." This means that a key can be used only if the two halves of the key, which are respectively stored in the terminal and the ROM key, are combined together successfully.

If a user fails to carry the ROM key, according to the teaching of the *Schneier* reference, this would create a problem in that the user cannot decrypt a cipher text since the user can obtain only one half of the key stored in the terminal and cannot complete the key required for decrypting the cipher text, because the user is missing the other half of the key stored in the ROM key.

On the other hand, according to the invention of Claim 17 of the present application, each of the key storage medium and the memory unit holds complete key information (the key information held by the memory unit is encrypted information).

With this construction of the present invention, if the user fails to carry the key storage medium, the user can still decrypt a cipher text using the key information stored in the memory unit.

Patent
62478-9100

As apparent, Claim 17 of the present application provides an advantageous effect over the *Schneier* reference, due to a switch unit and its operations which is not disclosed in the *Schneier* reference.

As can be appreciated, the same novel features is set forth in the other independent Claim 62, and accordingly, Claims 17 and 62 and their dependent claims are believed to constitute patentable subject matter.

Since the present invention narrows the issues for appeal, it is respectfully requested that this Rule 116 amendment be entered for those purposes alone. It is believed, however, that the present invention is now allowable over the reference of record.

If a telephone interview will help further the prosecution of this case, the Examiner can contact the undersigned attorney at the listed phone number.

I hereby certify that this correspondence is being transmitted via facsimile to the USPTO at 571-273-8300 on October 14, 2005.
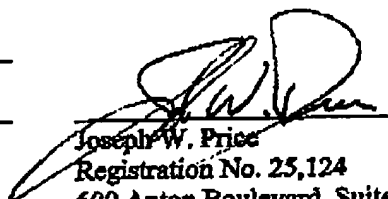
Very truly yours,

SNELL & WILMER L.L.P.

By: _____Sharon Farnus_____

Signature

Dated: October 14, 2005

Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420

62478.9100\PRICE\DRV\445321

13